Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/ot-security-readiness-checklist/

READINESS CHECKLIST

OT Security Readiness: Inventory, Boundaries and Rules Before Testing

A control network is assessed on its own terms, starting from an inventory the plant trusts, and that inventory is what lets the network be defended and audited. This checklist is what plant engineering, network and compliance assemble before any sensor is connected.

Why the Inventory and Stop Condition Come First

A well prepared operational technology assessment answers two concerns at once. The plant manager rightly keeps scanners away from a thirty year old controller, and the assessment respects that with a method built on passive capture, records and walkdowns. The process stays protected because active probes are kept away from fragile network stacks, human machine interfaces and anything that could trip the process. Both rest on the same preparation. The inventory tells everyone which assets are off limits. The signed stop condition and a named engineer who can halt the work give the plant a clear way to act when something unexpected happens. Our guide to scoping OT security testing around operational risk describes the rules of engagement a plant signs before anything touches the network.

The inventory is the foundation for the compliance file as well as the engineering work. NERC CIP-002 requires bulk electric system operators to identify and categorize their cyber systems before any later standard applies. Community water systems completing risk and resilience assessments under AWIA Section 2013 must assess the risks to their electronic and automated systems, which starts with knowing what they are. NIST SP 800-82 Revision 3 places asset management at the base of an OT security program. A listed controller is one the plant can patch, monitor and submit, and our guide to passive first asset discovery explains how the inventory is built from what the network actually shows and what the cabinets actually hold. The readiness items below are what the plant assembles so that work can begin safely.

The Order of Readiness, From Drawings to Signed Rules

Start with what the plant already has. The control engineer gathers the PLC project files, HMI tag databases, the existing asset spreadsheet and the maintenance records of field replacements, because those records bring the spreadsheet up to date with every device swapped in the field. Network engineering produces the as built drawings, the switch inventory with mirror capability noted, the firewall and jump host configurations and the list of vendor remote access paths. From those, the engineering team and the security lead draw the zones and conduits, mark each asset's operational criticality and name the ones that are off limits to any active technique, beginning with safety instrumented systems, turbine and generator controls, chemical dosing and anything whose failure has a physical consequence.

© 2026 Global Digital Forensics, Inc. All rights reserved.

With the picture drawn, the operational items follow. Operations identifies the maintenance windows in which any active work may occur and the operating modes the capture must cover, including startup, normal production, shift change and scheduled vendor maintenance. Network engineering identifies the SPAN or tap points that will see the most conduits and confirms each switch can mirror without affecting its own performance, noting unmanaged switches and serial segments as walkdown targets from the start so the walkdown covers them. The plant manager names the engineer who holds stop authority on the floor. Compliance maps the engagement to the mandate that governs it. All of that goes into a rules of engagement document that the plant manager, the control engineer and the corporate security lead sign together. Operators drafting one for the first time can begin with our OT audit workbook builder (evestigate.com/tools/ot-workbook-builder/).

Who Owns the Process, the Network and Stop Authority

The plant manager owns the process and the final word on what may be touched and when. The control engineer owns the asset classification and the project files. Network engineering owns the drawings, the switch configurations and the capture points. The corporate security lead owns the enterprise side of the boundary, the jump hosts, the firewalls and the vendor gateways where controlled active testing is appropriate, and coordinates with the plant rather than directing it. The compliance lead owns the mapping to CIP, AWIA, Coast Guard or other mandates and the submission calendar. The assessor owns the method, within the boundaries the plant has approved in writing.

Stop authority belongs to one named person on the plant floor, reachable for every active step, who can halt the work on their own authority. That person sits on the operations side, apart from the assessor and the corporate security lead, because the role answers to the process rather than to the engagement. Every person who acts is named in the agreed plan. Scans stay in the Purdue levels the plan assigns them, however quiet the capture looks. Vendor technicians keep to the work scheduled for the window. Assessors apply each technique to the segments the rules include. Every deviation from the plan is recorded, and a change to the plan is signed the same way the plan was.

How Planning Protects the Plant and the Assessment

GDF builds the OT assessment plan around the plant’s architecture, asset criticality and operating conditions. Our engineers use approved telemetry analysis, offline configuration review and site walkdowns, with active validation planned for the specific assets, methods and windows authorized by operations and engineering.

Coverage takes the same care. Capture points are chosen across the network, and walkdowns reach the serial links, unspanned VLANs, unmanaged switches and devices behind protocol gateways that sit outside the view of a single core switch. The inventory arrives with a coverage map, so every reader can see which segments were observed and for how long. The spreadsheet becomes the baseline once it is reconciled against project files and a cabinet walkdown, which brings years of field replacements into the record. And the engagement starts with an agreed goal, whether a first boundary picture, validation of a segmentation project or evidence for a specific submission, so the work is aimed squarely at that question. The OT assessment planning library holds the sector manuals that feed each of these decisions.

© 2026 Global Digital Forensics, Inc. All rights reserved.

How GDF Supports Plant Engineering, Security Leads and Compliance Teams

Global Digital Forensics has performed security assessments and forensic examinations since 1992, and our SCADA, ICS and OT security assessments are scoped around physical safety and operational continuity with the plant's engineers in control. In higher Purdue zones we perform controlled, manual attack path validation to see whether an intruder can cross into the industrial zone. In the lower levels we switch to passive telemetry at SPAN ports and taps, offline configuration review and maintenance window inspections. Every engagement begins with the rules of engagement described above, and the inventory we deliver records the source and confidence of every entry alongside a coverage map showing which segments were instrumented and for how long, so a maintenance engineer, a security lead and a compliance lead can each see how much weight an entry will bear.

The report is written for the mandate that governs the plant as well as for the engineering team, with findings expressed as the gap between the protection a zone has and the protection its risk requires in ISA/IEC 62443 terms, and mapped to the CIP standard, AWIA assessment or Coast Guard requirement the compliance lead must answer. Where an incident has already occurred, the same examiners preserve and analyze the record under the direction of counsel. Our clients include Fortune 1000 companies, and the initial consultation is free. If a mandate's submission is approaching and the inventory is a spreadsheet the plant wants confirmed, call (800) 868-8189 and a senior assessor will work through the readiness items with your plant engineer on the first call.

© 2026 Global Digital Forensics, Inc. All rights reserved.

The Checklist at a Glance

The readiness items a plant assembles before an OT security assessment, who owns each one, where it lives and how quickly it goes stale.

Item	Who acts	Where it lives	How fast it expires
Asset inventory with source and confidence	Control engineer with maintenance	PLC project files, HMI tag databases, walkdown notes	Drifts with every field replacement
Network drawings and conduits	Network engineering	As built drawings and switch configurations	Stale after any unrecorded change
Off limits assets and safety boundaries	Plant manager and control engineer	Rules of engagement, listed by Purdue level	Fixed for the engagement, renewed each time
SPAN or tap capture points	Network engineering	Managed switch mirror sessions and optical taps	Capture covers the segments and windows instrumented
Maintenance windows for active work	Operations manager	Outage and maintenance calendar	Set by the outage cycle
Stop authority	Named plant floor engineer	Rules of engagement and the contact sheet	Reachable for every active step
Vendor remote access inventory	IT and OT jointly	Firewall rules, jump hosts and vendor gateways	Changes whenever a vendor contract changes
Regulatory mapping	Compliance lead	CIP-002 categorization, AWIA assessment, Coast Guard plan	Each mandate runs its own submission cycle

FREQUENTLY ASKED

Questions Counsel Ask About This Checklist

Will the assessment require downtime?

The lower levels of the control network are assessed with passive capture, offline configuration review and walkdowns, all of which run while the plant operates. Any active technique is limited to the higher zones on the enterprise side of the boundary and to maintenance windows the plant chooses, under rules of engagement the plant manager and control engineer sign. A named engineer on the floor can halt the work at any time, and that authority is written into the document.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Our asset list is a spreadsheet. Is that enough to start?

It is enough to start the readiness work, and reconciliation brings it up to date. The spreadsheet is reconciled against PLC project files, HMI tag databases, maintenance records and a cabinet walkdown, and the capture then shows what is actually talking on the network. The resulting inventory records the source and confidence of each entry and a coverage map of where and when the capture observed the network, which is what a CIP auditor or AWIA certifier expects to see.

Who should hold stop authority?

A named engineer on the plant floor who answers to the process rather than to the engagement, and who can halt any step on their own authority. The role is written into the rules of engagement with contact details, and the person is reachable for every active step. The role sits apart from the assessor and the corporate security lead, because its value is its independence from both of them.

Which mandates does the assessment map to?

It depends on the sector. Bulk electric operators map to NERC CIP, with CIP-002 categorization and CIP-010 vulnerability assessment and baseline requirements. Community water systems map to AWIA Section 2013 risk and resilience assessments. Maritime operators map to Coast Guard cybersecurity requirements. NIST SP 800-82 and ISA/IEC 62443 supply the method and the zone model across all of them, and the compliance lead identifies which apply during readiness.

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.